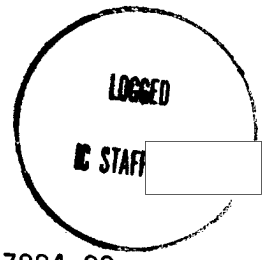
COLL 17-SR

DIRECTOR OF CENTRAL INTELLIGENCE
Intelligence Information Handling Committee
WASHINGTON, DC 20505



STAT

ICS 7884-88
9 November 1988

STAT MEMORANDUM FOR:

Joint Maritime Information Element (JMIE)
Program Management Office

SUBJECT: JMIE Security Requirement

1. The JMIE Implementation Board (JIB) has telephonically reviewed and approved the attachment requirement to control access to selected data stored in the JMIE Support System (JSS) central files by assignment of user priveleges. Most of the data contributed to the JSS will be available for open dissemination to all users holding secret clearances. However, in selected instances, information provided to JMIE will have special handling caveats attached to permit only those users who are authorized access to view the data.

2. Although information currently incorporated in the JSS testbed requires no special controls, the consortium strongly endorses designing the JCC and FOC systems to permit access priveleges and controlled dissemination of sensitive data. Therefore, request that the attached requirement, which expands on the Security and Privacy Requirements as stated in the JMIE Phase I Report, be reviewed for technical/cost considerations and incorporation into JCC/FOC and the results of those activities be provided to the JIB.

STAT

Chairman

Attachment:
As Stated

SUBJECT: JMIE Security Requirement

Distribution: ICS 7884-88
Orig - Adse
1 - IHC Subj
1 - IHC Chrono
1 - ICS Reg

STAT DCI/ICS/IHC/ [redacted] (9Nov88)

STATEMENT OF JCC REQUIREMENT - RESTRICTED DATA ACCESS

A Consortium requirement has been identified for restricting access to particular data maintained in the JSS Central files. The JCC Central database and access mechanisms must be designed to accommodate this requirement.

Some classes of source data input to the JSS will contain caveats describing special handling required in dealing with the material. Certain of these caveats will restrict read access of the data to particular JSS users. For these classes of source data, only those users who are authorized read access to that particular class shall be allowed to retrieve the data.

Each record stored in the JSS Central files shall contain a caveat field. This field shall be blank when the record is derived from non-caveated source data and shall otherwise be set to reflect the caveat of data input.

When a user is initially registered on the system, he or she shall be assigned a password and identification code along with a set of permissions regarding read and write privileges. The system shall maintain a record of these privileges associated with each user identification.

When a user queries the central files, the system shall ensure that only records for which he or she has access privilege are returned to the workstation. If a query has selected records for which a user is not privileged, the system shall so notify the user.